UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,648	06/25/2003	Dennis Morgan	M1103.70154US00	4051

45840 7590 05/20/2008

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
05/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,648	MORGAN ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33,37 and 39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33,37 and 39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Remarks filed on February 29, 2008.

Applicant has filed a Request for Continued Examination on October 5, 2007.

Claims 1-33 and 37-39 were rejected on November 29, 2007.

Claims 1, 19, 21, 24, and 37 have been amended. Claim 38 has been cancelled.

Claims 1-33, 37, and 39 are currently pending.

Response to Arguments

1. Applicant's arguments filed February 29, 2008 have been fully considered but they are not persuasive.

Applicant respectfully contends that Coley, in view of Montenegro does not teach all the limitations of claim 1. Specifically, Coley does not teach the part of a computer-implemented method, comprising: receiving, ***by an operating system and/or an enforcement module which is associated with or is part of the operating system***, a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection; and making, ***by the operating system and/or the enforcement module***, a call to a firewall to establish the connection in accordance with the parameters as presented by the Examiner. The Applicant argues that Coley discloses that the proxy agent assigned to a port performs

all of the verification processes and management of the port ***without involving the operating system***, or a port manager (as in conventional system) [Coley 7: 47-50]. In contrast claim 1 recites receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application.

The Examiner respectfully disagrees. In Coley, Col 7, Ln 47-50, disclosing that the part of the firewall application, called the proxy agent, that performs "all of the verification processes and management of the port without involving the operating system, or a port manager (as in conventional system)" does not mean that the firewall application receiving a call is not associated with or is part of the operating system. It means that the firewall application does not use conventional chained processes involving operating system based verification routines and port management that are generic to incoming access requests as normally used in conventional systems [Coley 7: 57-63]. Otherwise, the operating system is still associated or is part in running and supporting the processes of the firewall application. In fact, Coley teaches that the firewall application is associated with or is part of the operating system when Coley explicitly discloses that "the processes, programs, and applications running on the firewall computing platform are those ***involved with firewall process, or their support (ie. the computer's operating system)***" [Coley 7: 27-30].

Applicant respectfully contends that with regard to claim 21 as amended, Malcolm describes that the firewall receives the at least one access request definition from the application program [Malcolm 4: 20-22], while claim 21 recites receiving, by an interception module communicating with a firewall via a first application programming interface ... a connect attempt, a listen attempt, or a combination thereof from an application or a service. Furthermore, Malcolm describes that the firewall program accesses its access rules data structure and determines whether there is already an access rule covering the type of access request received from the application [Malcolm 9: 38-41]. Malcolm does not teach or suggest "receiving, by an interception module communicating with a firewall via a first application programming interface and including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module, and a filter cache, a connect attempt, a listen attempt, or a combination thereof from an application or a service; ...

The Examiner respectfully disagrees. The Examiner still cites Malcolm, Col 5, Ln 60-65, to teach the interception module communicating with a firewall via a first application programming interface and including a second application programming interface for at least one of a user, an application, and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module. Malcolm encompasses the Applicant's interception module because Malcolm's firewall program teaches all the limitations of the Applicant's interception module. Applicant's

programming interfaces are inherent in all programs utilizing function routines, program modules, or objects. Programming interfaces are necessary for the different functions, routines, programs, objects to interact with one another. Malcolm, Col 5, Ln 60-65 discloses that the firewall is able to intercept access requests which reads on the Applicant's "interception" module. Malcolm, Col 6, Ln 33-51 teaches that the firewall program also provides for a second application programming interface for at least one of a user, an application, and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module by disclosing that "an application program will preferably provide the firewall program with a list of Internet access requests that the application may possibly have during execution of the application..." These access requests establish at least one policy or access rules stored in a database or other suitable record management system or data structure associated with the firewall program [Malcolm 7: 21-30]. By showing that Malcolm's firewall program teaches the Applicant's limitations regarding the interception module also shows the interception module being encompassed in Malcolm's invention.

2. Applicant's amendments, see Amendments, filed February 29, 2008, with respect to claim 24 have been fully considered and are persuasive. The rejection of claim 24 under USC 112 has been withdrawn.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1-5, 7-15, and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. [US 5826014], hereinafter Coley, and further in view of Montenegro [US 6233688 B1].

Regarding claim 1, Coley teaches a computer-implemented method, comprising: receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system [US 5826014, Col 7, Ln 5-20], a call [US 5826014, Col 7, Ln 37] from an application, the call having parameters for a connection to an endpoint that the application desires to establish [US 5826014, Col 8, Ln 6-12], whereby the application explicitly communicates a request to traverse a firewall to establish the connection [US 5826014, Col 8, Ln 3-4 -- Examiner notes that a reliable request by the application would have meant that the application "explicitly" communicated a request which required only a minimum requirement verification before being connected as cited.]; and making, by the operating system and/or the enforcement module [US 5826014, Col 6, Ln 9-11], a call to the firewall to establish the connection in accordance with the parameters [US 5826014, Col 10, Ln 35-39].

Coley does not explicitly teach an application programming interface. Montenegro teaches a firewall traversal method regarding loading an application programming interface (API) onto the client system [US 6233688 B1, Col 7, Ln 17-20].

It would have been obvious to one of ordinary skilled in the art at the time of invention to implement an application programming interface as taught by Montenegro. The suggestion/motivation for implementing an application programming interface would have been to provide an interface between applications and the operating system achieving a form of standardization for applications to interface with the operating system. Montenegro is an analogous art because it solves the problem by providing the means of an interface between applications and an operating system.

Regarding claim 2, Coley and Montenegro teaches the method of claim 1, further comprising, at the firewall, evaluating the parameters with respect to a policy [US 5826014, Col 7, Ln 65-67 -- Examiner notes that a proxy agent being able to distinguish from a set of verification tests whose rigorousness is dictated by the characteristics of the application access request is evidence of a policy being used.] and, if the parameters meet the policy, establishing the network connection in accordance with the parameters [US 5826014, Col 9, Ln 1-31] [US 5826014, Col 10, Ln 35-39].

Regarding claim 3, Coley and Montenegro teaches the method of claim 1, wherein the parameters comprise a known endpoint to which the application would like to be connected [US 5826014, Col 10, Ln 3-5].

Regarding claim 4, Coley and Montenegro teaches the method of claim 3, wherein the parameters further comprise a request to limit the connection to a single connection [US 5826014, Col 9, Ln 34 – Examiner notes the validity check of one or more specific source addresses reads on limiting to a single connection.].

Regarding claim 5, Coley and Montenegro teaches the method of claim 4, further comprising, after the connection has been established, closing the connection in accordance with the request [US 5826014, Col 12, Ln 59-61].

Regarding claim 7, Coley and Montenegro teaches the method of claim 1, wherein the parameters comprise limiting the connection to a subset of interfaces, local addresses, or remote addresses, or combinations thereof [US 5826014, Col 9, Ln 33-36].

Regarding claim 8, Coley and Montenegro teaches the method of claim 1, wherein the parameters comprise a timeout policy for the connection [US 5826014, Col 9, Ln 61-67].

Regarding claim 10, Coley and Montenegro teaches the method of claim 1, wherein the

parameters comprise information about a property of a flow that requires special handling [US 5826014, Col 11, Ln 54-55].

Regarding claim 11, Coley and Montenegro teaches the method of claim 10, wherein the information comprises a request for authentication or encryption handling [US 5826014, Col 11, Ln 54-55 – Examiner notes that the necessity of password information reads on authentication.].

Regarding claim 12, Coley and Montenegro teaches the method of claim 1, wherein the application explicitly communicates the request to establish the connection by opening a listening socket [US 5826014, Col 6, Ln 5-7 -- Examiner notes that is inherent for each proxy agent to open a listening socket to its designated port to monitor incoming access requests from an application explicitly communicating a request to establish a connection.].

Regarding claim 13, Coley and Montenegro teaches the method of claim 1, wherein the application explicitly communicates the request to establish the connection by connecting to a socket [US 5826014, Col 7, Ln 42 -- Examiner notes that a request attaching to a particular port is evidence that the application explicitly communicating a request to establish a connection connects to a particular socket that was opened by a particular proxy agent.].

Regarding claim 14, Coley and Montenegro teaches the method of claim 1, wherein the call to the firewall is made via a firewall application programming interface [Examiner notes that an application interface is inherent in any kind of communication between applications.].

Regarding claim 15, Coley and Montenegro teaches the method of claim 1, wherein the firewall is located on a computer with the application [US 5826014, Col 7, Ln 24-34].

Claims 18 and 19 are rejected because it is directed to the same subject matter as claim 1.
Claim 20 is rejected because it is directed to the same subject matter as claim 14.

2. Claims 21-26, 30, 33, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm [US 7146638 B2], and further in view of Montenegro [US 6233688 B1].
Regarding claim 21, Malcolm teaches a computer-implemented method, comprising: receiving, by an interception module communicating with a firewall via a first application programming interface [US 7146638 B2, Col 5, Ln 60-65 – Examiner notes that intercepting access requests from application program is evidence of an interception module.] and including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies [Malcolm 6: 33-51] stored in a policy cache of the interception module [Malcolm

7: 21-30], and a filter cache [US 7146638 B2, Col 7, Ln 36-41 -- Examiner notes the retrieval of a configuration of granting/deny access requests based from comparing access request parameters with the access rules is evidence of a filter cache.], a connect attempt, a listen attempt, or a combination thereof from an application or a service [US 7146638 B2, Col 7, Ln 51-59]; extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof [US 7146638 B2, Col 4, Ln 26-37]; identifying, by the interception module, the user and the application or the service from the user and application or service information [US 7146638 B2, Col 4, Ln 26-37]; evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies [US 7146638 B2, Col 7, Ln 36-41]; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, by the interception module, a firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache [US 7146638 B2, Col 9, Ln 38-52 – Examiner notes that approving/denying of access requests based from evaluating access requests against access rules that covers such requests is evidence that configurations have been created for those requests. Examiner also notes that access rules read on firewall policies.].

Malcolm does not explicitly teach an application programming interface. Montenegro teaches a firewall traversal method regarding loading an application programming interface (API) onto the client system [US 6233688 B1, Col 7, Ln 17-20].

It would have been obvious to one of ordinary skilled in the art at the time of invention to implement an application programming interface as taught by Montenegro. The suggestion/motivation for implementing an application programming interface would have been to provide an interface between applications and the operating system achieving a form of standardization for applications to interface with the operating system. Montenegro is an analogous art because it solves the problem by providing the means of an interface between applications and an operating system.

Regarding claim 22, Malcolm and Montenegro teaches the method of claim 21, further comprising if the connect attempt, the listen attempt, or the combination thereof do not comply with one or more policies from the plurality of policies, sending a notification to the user of the application or service [US 7146638 B2, Col 9, Ln 53-59].

Regarding claim 23, Malcolm and Montenegro teaches the method of claim 22, wherein the notification comprises a selection to allow a connection [US 7146638 B2, Col 9, Ln 59].

Regarding claim 24, Malcolm and Montenegro teaches the method of claim 21, wherein establishing the at least one policy comprises receiving a policy from the application or

service [US 7146638 B2, Col 4, Ln 26-37] [Examiner notes for examining purposes, establishing the policy is interpreted as providing all access rules/requirements by the application program as cited.].

Regarding claim 25, Malcolm and Montenegro teaches the method of claim 24, wherein receiving the policy comprises receiving the policy via the application programming interface [An application programming interface would have been inherent.].

Regarding claim 26, Malcolm and Montenegro teaches the method of claim 24, wherein the policy received from the application or service comprises inbound or outbound restrictions using one or more Internet Protocol addresses, information about a subnet, information about scope of the connection, or combinations thereof [US 7146638 B2, Col 4, Ln 28-37].

Regarding claim 30, Malcolm and Montenegro teaches the method of claim 21, wherein the firewall comprises a host firewall located on a computer with the application [US 7146638 B2, Fig 1, Itm 24].

Claim 33 and 37 are rejected as directed to the same subject matter as claim 21.

3. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. [US 5826014], hereinafter Coley, Montenegro [US 6233688 B1], and further in view of Hedge et al. [US 6925495 B2], hereinafter Hedge.

Regarding 6, Coley and Montenegro teaches the method of claim 1. But Coley and Montenegro does not teach wherein the parameters comprise a request for bandwidth or connection throttling for the connection.

Hedge teaches a computer-implemented method, comprising: receiving a call from an application [US 6925495 B2, Fig 5, Itm 510 – Examiner notes that an application is inherent in a requesting device], the call having parameters for a connection to an endpoint that the application desires to establish [US 6925495 B2, Fig 8], whereby the application explicitly communicates a request to establish the connection and making a call to a firewall to establish the connection in accordance with the parameters [US 6925495 B2, Col 13, Ln 22-31], wherein the parameters comprise a request for bandwidth or connection throttling for the connection [US 6925495 B2, Col 16, Ln 10-11].

It would have been obvious to one of ordinary skill in the art at the time of invention to accommodate a request for bandwidth or connection throttling as one of the parameters as taught by Hedge. The suggestion/motivation for the accommodation of bandwidth request is that since many sites rely on the user having a high bandwidth when streaming media to the user, bandwidth allocation is needed in a firewall to optimize content delivery [US 6925495 B2, Col 1, Ln 47-50]. Hedge is an analogous art because Hedge solves the problem of optimizing content delivery over a network by requesting and accommodating bandwidth allocation.

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. [US 5826014], hereinafter Coley, Montenegro [US 6233688 B1], and further in view of Keane et al. [US 2003/0131263 A1], hereinafter Keane.

Regarding claim 9, Coley and Montenegro teaches the method of claim 1. But Coley and Montenegro does not teach wherein the parameters comprise turning off or on specific protocol options.

Keane teaches a computer-implemented method, comprising: receiving a call [US 2003/0131263 A1, Fig 8, Itm 800 – Examiner notes that receiving packets to be transported across a network is evidence of receiving a call.] from an application [US 2003/0131263 A1, Pg 6, Par 0066 -- Examiner notes that network interfaces are application interface receiving the packets.], the call having parameters for a connection to an endpoint that the application desires to establish [US 2003/0131263 A1, Fig 6,7], whereby the application explicitly communicates a request to establish the connection and making a call to a firewall to establish the connection in accordance with the parameters [US 2003/0131263 A1, Pg 7, Par 0081], wherein the parameters comprise turning off or on specific protocol options [US 2003/0131263 A1, Pg 7, Par 0084].

It would have been obvious to one of ordinary skill in the art at the time of invention to accommodate the specific protocol options as taught by Keane. The

suggestion/motivation for the accommodation of specific protocol options is to provide information to the firewall for evaluation of a packet whose specific protocol options may be set [US 2003/0131263 A1, Pg 7, Par 0084]. Keane is an analogous art because Keane is in the same field of transmitting packet content across a network using firewall modules.

5. Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. [US 5826014], hereinafter Coley, Montenegro [US 6233688 B1], and further in view of Chen [US 7000006 B1].

Regarding claim 16, Coley and Montenegro teaches the method of claim 1. But Coley and Montenegro do not teach wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection.

Chen teaches a computer-implemented method, comprising: receiving a call from an application via an application programming interface and making a call to a firewall to establish the connection [US 7000006 B1, Col 9, Ln 21-29], wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection [US 7000006 B1, Col 9, Ln 21-29 -- Examiner notes that intercepting communications to a corresponding secure domain is evidence of an application agent providing such functions.].

It would have been obvious to one of ordinary skill in the art at the time of invention to implement edge firewalls as taught by Chen. The suggestion/motivation for combining Chen would have been to reduce the amount of processing time involved in configuring networks for policy managements [US 7000006 B1, Col 1, Ln 40-47] because the network can be abstracted into domains thus having reduced topology and internal connectivity [US 7000006 B1, Col 1, Ln 51-59] which is made possible by implementing edge firewalls. Chen is an analogous art because Chen solves the problem of being able to reduce the amount of processing time involved in configuring networks for policy managements.

Regarding claim 17, Coley, Montenegro, and Chen teach the method of claim 1, wherein the firewall comprises an edge firewall [US 7000006 B1, Col 9, Ln 21-29], and further comprising an authenticated protocol [US 7000006 B1, Col 2, Ln 65-67 -- Examiner notes authentication modules is evidence of authenticated protocols.] to communicate information to the edge firewall about the connection.

6. Claims 31, 32, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm [US 7146638 B2], Montenegro [US 6233688 B1], and further in view of Chen [US 7000006 B1].

Regarding claim 31, Malcolm and Montenegro teaches the method of claim 21. But Malcolm and Montenegro do not teach wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information about the connection.

Chen teaches a computer-implemented method, comprising: receiving a connect attempt, a listen attempt, or a combination thereof from an application or a service [US 7000006 B1, Col 9, Ln 24-25]; evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies [US 7000006 B1, Col 9, Ln 11-15]; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, by the interception module, a firewall to allow the connect attempt, the listen attempt, or the combination thereof [US 7000006 B1, Col 3, Ln 10-13], wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection [US 7000006 B1, Col 9, Ln 21-29 -- Examiner notes that intercepting communications to a corresponding secure domain is evidence of an application agent providing such functions.].

It would have been obvious to one of ordinary skill in the art at the time of invention to implement edge firewalls as taught by Chen. The suggestion/motivation for combining Chen would have been to reduce the amount of processing time involved in configuring networks for policy managements [US 7000006 B1, Col 1, Ln 40-47] because the

network can be abstracted into domains thus having reduced topology and internal connectivity [US 7000006 B1, Col 1, Ln 51-59] which is made possible by implementing edge firewalls. Chen is an analogous art because Chen solves the problem of being able to reduce the amount of processing time involved in configuring networks for policy managements.

Regarding claim 32, Malcolm, Montenegro, and Chen teach the method of claim 21, wherein the firewall comprises an edge firewall [US 7000006 B1, Col 9, Ln 21-29], and further comprising an authenticated protocol [US 7000006 B1, Col 2, Ln 65-67 -- Examiner notes authentication modules is evidence of authenticated protocols.] to communicate information to the edge firewall about the connection.

Claim 39 is rejected because it is the system performing the method of claim 31.

7. Claims 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm [US 7146638 B2], Montenegro [US 6233688 B1], and further in view of Keane et al. [US 2003/0131263 A1], hereinafter Keane.

Regarding claim 27, Malcolm and Montenegro teach the method of claim 24. But Malcolm and Montenegro does not teach wherein the policy received from the application or service comprises communication security level.

Keane teaches a computer-implemented method, comprising: receiving a connect attempt, a listen attempt, or a combination thereof from an application or a service [US 2003/0131263 A1, Fig 8, Itm 800]; evaluating, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies [US 2003/0131263 A1, Pg 7, Par 0081],wherein establishing the policy comprises receiving a policy from the application or service [US 2003/0131263 A1, Pg 5, Par 0061-0062],wherein the policy received from the application or service comprises communication security level [US 2003/01321263 A1, Pg 3, Par 0040] [US 2003/0131263 A1, Pg 4, Par 0042]; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, a firewall to allow the connect attempt, the listen attempt, or the combination thereof [US 2003/0131263 A1, Pg 7, Par 0080].

It would have been obvious to one of ordinary skill in the art at the time of invention to accommodate policies with communication security levels as taught by Keane. The suggestion/motivation for the accommodation of communication security levels as part of the policies is to provide secure private connections over the Internet by enabling authentication of users and locations and encryption of communication, thereby delivering secure and private "tunnels" between users or locations and thus establishing a virtual private network, or VPN [US 2003/0131263 A1, Pg 1, Par 0009]. Keane is an analogous art because Keane is in the same field of transmitting packet content across a network using firewall modules.

Regarding claim 28, Malcolm, Montenegro, and Keane teach the method of claim 27, wherein the communication security level comprises authentication [US 2003/0131263 A1, Pg 4, Par 0042].

Regarding claim 29, Malcolm, Montenegro, and Keane teach the method of claim 27, wherein the communication security level comprises encryption [US 2003/01321263 A1, Pg 3, Par 0040].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132